1変数多項式の再帰的な多項式剰余列と入れ子部分終結式 (Computer Algebra : Design of Algorithms, Implementations and Applications)

AUTHOR(S):

照井, 章

CITATION:

照井, 章. 1変数多項式の再帰的な多項式剰余列と入れ子部分終結式 (Computer Algebra : Design of Algorithms, Implementations and Applications). 数理解析研究所講究録 2006, 1514: 87-93

ISSUE DATE:

2006-09

URL:

http://hdl.handle.net/2433/58679

数理解析研究所講究録
1514巻 2006年 87-93

1変数多項式の再帰的な多項式剰余列と入れ子部分終結式

照井 章 *
AKIRA TERUI
筑波大学大学院数理物質科学研究科
GRADUATE SCHOOL OF PURE AND APPLIED SCIENCE, UNIVERSITY OF TSUKUBA

Abstract

本稿では, 1変数多項式の部分終結式の拡張の一つである "再帰的な部分終結式 (recursive subresultant)" の新たな表現として "入れ子部分終結式 (nested subresultant)" および "簡約入れ子部分終結式 (reduced nested subresultant)" を与える. 簡約入れ子部分終結式は, その行列の次元が, 最初に著者が提案した再帰的な部分終結式の行列ひ比べて大幅に小さくなり, 再帰的な多項式剰余列に基づく種々の計算が容易になる.

1 はじめに

多項式剰余列 (PRS) は数式処理における基本的な道具の一つである. 多項式剰余列の算法として知られているEuclidの互除法 [4] は単純であるが, 係数膨張が計算効率上の問題となる. この問題の解決策として, 係数膨張の仕組みが詳しく調べられ, 部分終結式の理論が発展してきた (Brown and Traub [2], Collins [3], Loos [5] 等を参照). 部分終結式の理論を用いることにより, 多項式剰余列の要素に現われる余分な因子を系統的に取り除き, 係数膨張を抑制することが可能になる.

著者は, これまでの研究で, 多項式剰余列の一つの拡張として "再帰的な多項式剰余列 (recursive PRS)", および, それに対応する部分終結式として "再帰的な部分終結式 (recursive subresultant)" をそれぞれ提案した ([6], [9]). 再帰的な多項式剰余列は, 多項式剰余列の最後に初期多項式のGCDが現われた際に, それとその1階微分を入力として新しい多項式剰余列を生成し, 剰余が定数になるまで計算を繰り返すものである. 再帰的な多項式剰余列の各要素の係数は, 最初に与えられる多項式の係数に依存し, それらは再帰的な部分終結式によって表現することができる. しかし, 再帰の回数が深くなると, その部分終結式行列の次数は増大し, 部分終結式行列を用いた諸計算が実用に適さなくなる [9].

本稿では, 再帰的な多項式剰余列に対する部分終結式の新たな表現として "入れ子部分終結式 (nested subresultant)" および "簡約入れ子部分終結式 (reduced nested subresultant)" を与える. 入れ子部分終結式は, その係数が, 初期多項式の係数を要素とする行列式の入れ子で表され, 再帰的な部分終結式と簡約入れ子部分終結式の同値性を示すのに用いる. 簡約入れ子部分終結式は, その行列が, 入れ子部分終結式行列を分数なしGaussの消去法を用いて簡約したものと同値で, もとの再帰的な部分終結式行列に比べると次元が大幅に小さくなっており, 再帰的な多項式剰余列に基づく種々の計算が容易になる.

本稿では以下の内容を述べる. 第2章では再帰的な多項式剰余列と再帰的な部分終結式を復習する. 第3章では入れ子部分終結式を定義し, 再帰的な部分終結式との同値性を示す. 第4章では簡約入れ子部分終結式を定義し, これが入れ子部分終結式を簡約した表現であることを示す.

*terui@math.tsukuba.ac.jp

2 再帰的な多項式剰余列と再帰的な部分終結式

Rを整域, KをRの商体とし, FとGを$R[x]$の1変数多項式とする. FとGが自明でないGCDをもつ場合, 普通はそこで剰余列の計算を終えるが, そのGCDとその1階微分から新たな多項式剰余列を生成する計算が用いられる場合がある（無平方分解など）. このようにして計算される多項式剰余列を "再帰的な多項式剰余列" と呼ぶ.

以下では, 本稿の議論に必要な記号を定義し, 再帰的な多項式剰余列と再帰的な部分終結式の定義を復習する（証明などの詳細はTerui [6]を参照）.

2.1 再帰的な多項式剰余列

定義 1 (多項式剰余列 (PRS))
FとGを$R[x]$の1変数多項式とし, 次数をそれぞれm, n（ただし$m > n$）とする. このとき,

$$\begin{gathered} P_1 = F, \quad P_2 = G, \quad \alpha_i P_{i-2} = q_{i-1} P_{i-1} + \beta_i P_i \quad (i = 3, \ldots, l), \\ \alpha_i, \beta_i \in R, \quad \deg(P_{i-1}) > \deg(P_i) \end{gathered} \tag{1}$$

によって定義される多項式の列$(P_1, \ldots, P_l)$をFとGの**多項式剰余列** *(PRS)* といい, $\mathrm{prs}(F, G)$で表す. このとき, 列$((\alpha_3, \beta_3), \ldots, (\alpha_l, \beta_l))$を$\mathrm{prs}(F, G)$の *division rule* という（von zur Gathen and Lücking [8]を参照）. P_lが定数のとき, $\mathrm{prs}(F, G)$は**完全** *(complete)* であるという（Knuth [4]を参照）. ∎

定義 2 (再帰的な多項式剰余列 (Recursive PRS))
FとGを定義1で定義される多項式とする. このとき,

$$\begin{aligned} & P_1^{(1)} = F, \quad P_2^{(1)} = G, \quad P_{l_1}^{(1)} = \gamma_1 \cdot \gcd(P_1^{(1)}, P_2^{(1)}), \quad \gamma_1 \in R, \\ & (P_1^{(1)}, P_2^{(1)}, \ldots, P_{l_1}^{(1)}) = \mathrm{prs}(P_1^{(1)}, P_2^{(1)}), \\ & P_1^{(k)} = P_{l_{k-1}}^{(k-1)}, \quad P_2^{(k)} = \frac{d}{dx} P_{l_{k-1}}^{(k-1)}, \quad P_{l_k}^{(k)} = \gamma_k \cdot \gcd(P_1^{(k)}, P_2^{(k)}), \quad \gamma_k \in R, \\ & (P_1^{(k)}, P_2^{(k)}, \ldots, P_{l_k}^{(k)}) = \mathrm{prs}(P_1^{(k)}, P_2^{(k)}), \quad k = 2, \ldots, t \end{aligned} \tag{2}$$

によって与えられる多項式の列$(P_1^{(1)}, \ldots, P_{l_1}^{(1)}, P_1^{(2)}, \ldots, P_{l_2}^{(2)}, \ldots, P_1^{(t)}, \ldots, P_{l_t}^{(t)})$を$F$と$G$の**再帰的な多項式剰余列** *(recursive PRS)* といい, $\mathrm{rprs}(F, G)$で表す. このとき, 列$((\alpha_3^{(1)}, \beta_3^{(1)}), \ldots, (\alpha_{l_t}^{(t)}, \beta_{l_t}^{(t)}))$を$\mathrm{rprs}(F, G)$の *division rule* という. $P_{l_t}^{(t)}$が定数のとき, $\mathrm{rprs}(F, G)$は完全 *(complete)* であるという. ∎

以下では次の記法を用いる. $k = 1, \ldots, t$および$i = 1, \ldots, l_k$に対し, $c_i^{(k)} = \mathrm{lc}(P_i^{(k)})$, $n_i^{(k)} = \deg(P_i^{(k)})$, $j_0 = m$, $j_k = n_l^{(k)}$とおく. $k = 1, \ldots, t$および$i = 1, \ldots, l_k - 1$に対し, $d_i^{(k)} = n_i^{(k)} - n_{i+1}^{(k)}$とおく.

2.2 再帰的な部分終結式

ここでは, 再帰的な部分終結式の定義を与える. その係数は, 初めに与えるFとGの係数の要素とする行列式で表される.

FとGをそれぞれ次式で与えられる$R[x]$の多項式とする.

$$F(x) = f_m x^m + \cdots + f_0 x^0, \quad G(x) = g_n x^n + \cdots + g_0 x^0, \quad m \geq n > 0. \tag{3}$$

正方行列Mに対し, Mの行列式を$|M|$で表す.

定義 3 (Sylvester 行列, 部分終結式行列)
F と G を式 (3) で定義される多項式とする. このとき, F と G の係数から式 (4) の $N(F,G)$ によって定義される $(m+n)$ 次正方行列を **F と G の Sylvester 行列**という. $j<n$ に対し, $N(F,G)$ から F の係数部分の左側 $n-j$ 列と G の係数部分の左側 $m-j$ 列を取り出した小行列 (式 (4) の $N^{(j)}(F,G)$) を **F と G の j 次の部分終結式行列**という.

$$N(F,G)=\overbrace{\begin{pmatrix} f_m & & & g_n & & \\ \vdots & \ddots & & \vdots & \ddots & \\ f_0 & & f_m & g_0 & & g_n \\ & \ddots & \vdots & & \ddots & \vdots \\ & & f_0 & & & g_0 \end{pmatrix}}^{n\text{列}\quad m\text{列}},\quad N^{(j)}(F,G)=\overbrace{\begin{pmatrix} f_m & & & g_n & & \\ \vdots & \ddots & & \vdots & \ddots & \\ f_0 & & f_m & g_0 & & g_n \\ & \ddots & \vdots & & \ddots & \vdots \\ & & f_0 & & & g_0 \end{pmatrix}}^{n-j\text{列}\quad m-j\text{列}}. \tag{4}$$

∎

定義 4 (再帰的な部分終結式行列)
F と G を式 (3) で定義される多項式とし, $(P_1^{(1)},\dots,P_{l_1}^{(1)},\dots,P_1^{(t)},\dots,P_{l_t}^{(t)})$ を F と G の完全な再帰的多項式剰余列とする. このとき, 数の組 (k,j) (ただし $k=1,\dots,t$, $j=j_{k-1}-2,\dots,0$) に対し, 行列 $\bar{N}^{(k,j)}(F,G)$ を以下のように再帰的に定義する.

1. $k=1$ に対し, $\bar{N}^{(1,j)}(F,G)=N^{(j)}(F,G)$ とおく.
2. $k>1$ に対し, $\bar{N}^{(k,j)}(F,G)$ を以下の上ブロックと下ブロックからなる行列として定義する.
   (a) $\bar{N}^{(k-1,j_{k-1})}(F,G)$ の下 $j_{k-1}+1$ を取り除いた小行列を $\bar{N}_U^{(k-1,j_{k-1})}$ とおく. このとき, $\bar{N}_U^{(k-1,j_{k-1})}$ を左上部から対角線状に $(j_{k-1}-j_k-1)$ 個並べたブロックを上ブロックとする.
   (b) $\bar{N}^{(k-1,j_{k-1})}(F,G)$ の下 $j_{k-1}+1$ の小行列を $\bar{N}_L^{(k-1,j_{k-1})}$ とおき, $\bar{N}_L^{(k-1,j_{k-1})}$ の第 $j_{k-1}+1-\tau$ 行 $(\tau=j_{k-1},\dots,1)$ を τ 倍し, 最下行を除いた小行列を $\bar{N}_L^{'(k-1,j_{k-1})}$ とおく. このとき, $j_{k-1}-j-1$ 個の $\bar{N}_L^{(k-1,j_{k-1})}$ を最左部のブロックから 1 行ずつ右下がりになるように並べ, ついで $j_{k-1}-j$ 個の $\bar{N}_L^{'(k-1,j_{k-1})}$ を, 最左部のブロックの第 1 行を $\bar{N}_L^{(k-1,j_{k-1})}$ の最左部のブロックの第 1 行に合わせ, 以下 1 行ずつ右下がりになるように並べたものを下ブロックとする.

このとき, $\bar{N}^{(k,j)}(F,G)$ を F と G の (k,j) **次の再帰的な部分終結式行列**と呼ぶ. ∎

命題 5
$k=1,\dots,t$ および $j<j_{k-1}-1$ に対し, (k,j) 次の再帰的な部分終結式行列 $\bar{N}^{(k,j)}(F,G)$ の行数と列数は, それぞれ $(m+n-2j_1)\left\{\prod_{l=2}^{k-1}(2j_{l-1}-2j_l-1)\right\}(2j_{k-1}-2j-1)+j$ 行, $(m+n-2j_1)\left\{\prod_{l=2}^{k-1}(2j_{l-1}-2j_l-1)\right\}\times(2j_{k-1}-2j-1)$ 列である. ∎

定義 6 (再帰的な部分終結式)
F と G を式 (3) で定める. $(P_1^{(1)},\dots,P_{l_1}^{(1)},\dots,P_1^{(t)},\dots,P_{l_t}^{(t)})$ を F と G の完全な再帰的多項式剰余列とし, $j_0=m$, $j_k=n_l^{(k)}$ $(k=1,\dots,t)$ とおく. $j=j_{k-1}-2,\dots,0$ および $\tau=j,\dots,0$ に対し, $\bar{N}^{(k,j)}(F,G)$ の上部 $(m+n-2j_1)\{\prod_{l=2}^{k-1}(2j_{l-1}-2j_l-1)\}(2j_{k-1}-2j-1)-1$ 行と第 $(m+n-2j_1)\{\prod_{l=2}^{k-1}(2j_{l-1}-2j_l-1)\}(2j_{k-1}-2j-1)+j-\tau$ 行からなる小行列を $\bar{N}_\tau^{(k,j)}=\bar{N}_\tau^{(k,j)}(F,G)$ とおく ($\bar{N}_\tau^{(k,j)}$ は正方行列であることに注意). このとき, 多項式

$$\bar{\mathrm{S}}_{k,j}(F,G)=|\bar{N}_j^{(k,j)}|x^j+\cdots+|\bar{N}_0^{(k,j)}|x^0 \tag{5}$$

を F と G の (k,j) **次の再帰的な部分終結式**と呼ぶ. ∎

3 入れ子部分終結式

再帰的な部分終結式行列の次数は, 再帰の回数が深まるに従って急速に増大するので, 再帰的な多項式剰余列に基づく種々の計算への効率的な利用が困難になる. そこで, 再帰的な部分終結式と定数倍を除いて等しいような新たな部分終結式の表現を導入することにより, 部分終結式行列の計算の効率化を図る.

本章で定義する "入れ子部分終結式 (nested subresultant)" は, 主に, 再帰的な部分終結式と, 後で述べる簡約入れ子部分終結式の関係を示すのに用いる.

定義 7 (入れ子部分終結式行列 (Nested Subresultant Matrix))
F と G をそれぞれ式 (3) で与えられる多項式とし, $(P_1^{(1)},\ldots,P_{l_1}^{(1)},\ldots,P_1^{(t)},\ldots,P_{l_t}^{(t)})$ を F と G の完全な再帰的な多項式剰余列とする. このとき, 数の組 (k,j) (ただし $k=1,\ldots,t,\ j=j_{k-1}-2,\ldots,0$) に対し, 行列 $\tilde{N}^{(k,j)}(F,G)$ を以下のように再帰的に定義する.

1. $k=1$ に対し, $\tilde{N}^{(1,j)}(F,G)=N^{(j)}(F,G)$ とおく.
2. $k>1,\ \tau=0,\ldots,j_{k-1}$ に対し, $\tilde{N}^{(k-1,j_{k-1})}$ の上部 $(n_1^{(k-1)}+n_2^{(k-1)}-2j_{k-1}-1)$ 行および第 $(n_1^{(k-1)}+n_2^{(k-1)}-j_{k-1}-\tau)$ 行からなる小行列を $\tilde{N}_\tau^{(k-1,j_{k-1})}$ とおく ($\tilde{N}_\tau^{(k-1,j_{k-1})}$ は正方行列であることに注意). そして
$$\tilde{N}^{(k,j)}(F,G)=N^{(j)}\left(\tilde{\mathrm{S}}_{k-1,j_{k-1}}(F,G),\frac{d}{dx}\tilde{\mathrm{S}}_{k-1,j_{k-1}}(F,G)\right), \tag{6}$$
とおく. ここに, $\tilde{\mathrm{S}}_{k-1,j_{k-1}}(F,G)$ は定義 8 によって定義される多項式である.

このとき, $\tilde{N}^{(k,j)}(F,G)$ を F と G の (k,j) 次の入れ子部分終結式行列と呼ぶ. ∎

定義 8 (入れ子部分終結式 (Nested Subresultant))
F と G をそれぞれ式 (3) で与えられる多項式とし, $(P_1^{(1)},\ldots,P_{l_1}^{(1)},\ldots,P_1^{(t)},\ldots,P_{l_t}^{(t)})$ を F と G の完全な再帰的な多項式剰余列とする. そして, 数の組 (k,j) (ただし $k=1,\ldots,t,\ j=j_{k-1}-2,\ldots,0$) に対し, (k,j) 次の入れ子部分終結式行列 $\tilde{N}^{(k,j)}(F,G)$ の上部 $n_1^{(k)}+n_2^{(k)}-2j-1$ 行および第 $(n_1^{(k)}+n_2^{(k)}-j-\tau)$ 行からなる小行列を $\tilde{N}_\tau^{(k,j)}=\tilde{N}_\tau^{(k,j)}(F,G)$ とおく. このとき, 多項式
$$\tilde{\mathrm{S}}_{k,j}(F,G)=|\tilde{N}_j^{(k,j)}|x^j+\cdots+|\tilde{N}_0^{(k,j)}|x^0 \tag{7}$$
を F と G の (k,j) 次の入れ子部分終結式と呼ぶ. ∎

入れ子部分終結式は, 符号を除いて再帰的な部分終結式に等しいことが, 次の定理によって示される.

定理 9
F と G をそれぞれ式 (3) で与えられる多項式とし, $(P_1^{(1)},\ldots,P_{l_1}^{(1)},\ldots,P_1^{(t)},\ldots,P_{l_t}^{(t)})$ を F と G の完全な再帰的な多項式剰余列とする. $k=2,\ldots,t,\ j=j_{k-1}-2,\ldots,0$ に対し, $u_{k,j},\ b_{k,j},\ r_{k,j},\ R_k$ を次のように定義する:
$$\begin{aligned}
&u_{k,j}=(m+n-2j_1)\left\{\prod_{l=2}^{k-1}(2j_{l-1}-2j_l-1)\right\}(2j_{k-1}-2j-1),\quad u_k=u_{k,j_k},\quad u_1=m+n-2j_1,\\
&b_{k,j}=2j_{k-1}-2j-1,\quad b_k=b_{k,j_k},\quad b_1=1,\\
&r_{k,j}=(-1)^{(u_{k-1}-1)(1+2+\cdots+(b_{k,j}-1))},\quad r_k=r_{k,j_k},\quad r_{1,j}=1\quad (j<n),\\
&R_k=(R_{k-1})^{b_k}r_k,\quad R_0=R_1=1.
\end{aligned} \tag{8}$$
このとき,
$$\tilde{\mathrm{S}}_{k,j}(F,G)=(R_{k-1})^{b_{k,j}}\,r_{k,j}\,\bar{\mathrm{S}}_{k,j}(F,G) \tag{9}$$
が成り立つ. ∎

定理 9 は次の補題によって証明される.

補題 10
$k=1,\ldots,t,\ j=j_{k-1}-2,\ldots,0,\ \tau=j,\ldots,0$ に対し,

$$|\tilde{N}_{\tau}^{(k,j)}(F,G)| = (R_{k-1})^{b_{k,j}}\, r_{k,j}\, |\bar{N}_{\tau}^{(k,j)}(F,G)| \tag{10}$$

が成り立つ.

証明 Terui [7] を参照. ∎

4 簡約入れ子部分終結式

入れ子部分終結式は, その行列が部分終結式行列の行列式の入れ子の形（行列式の要素が別の行列式で表されるような形）で表現されるため, 実用に供することが困難である. しかし, 分数なし Gauss の消去法 [1] を用いることにより, 入れ子部分終結式の行列表現を, 行列式の入れ子でないような行列表現に変えることが可能な場合がある. その場合に簡約した行列から構成される部分終結式が, 簡約入れ子部分終結式である.

定義 11 (簡約入れ子部分終結式行列 (Reduced Nested Subresultant Matrix))
F と G をそれぞれ式 (3) で与えられる多項式とし, $(P_1^{(1)},\ldots,P_{l_1}^{(1)},\ldots,P_1^{(t)},\ldots,P_{l_t}^{(t)})$ を F と G の完全な再帰的な多項式剰余列とする. このとき, 数の組 (k,j) （ただし $k=1,\ldots,t,\ j=j_{k-1}-2,\ldots,0$） に対し, 行列 $\hat{N}^{(k,j)}(F,G)$ を以下のように再帰的に定義する.

1. $k=1$ に対し, $\hat{N}^{(1,j)}(F,G)=N^{(j)}(F,G)$ とおく.
2. $k>1$ に対し, $\hat{N}^{(k-1,j_{k-1})}(F,G)$ の下部 $j_{k-1}+1$ 行からなる小行列を $\hat{N}_L^{(k-1,j_{k-1})}(F,G)$, $\hat{N}^{(k-1,j_{k-1})}(F,G)$ から $\hat{N}_L^{(k-1,j_{k-1})}(F,G)$ を除いた小行列を $\hat{N}_U^{(k-1,j_{k-1})}(F,G)$ とおく. $\tau=j_{k-1},\ldots,0$ に対し, $\hat{N}^{(k-1,j_{k-1})}(F,G)$ から $\hat{N}_U^{(k-1,j_{k-1})}(F,G)$ と $\hat{N}_L^{(k-1,j_{k-1})}(F,G)$ の第 $(j_{k-1}-\tau+1)$ 行を取り出した小行列を $\hat{N}_{\tau}^{(k-1,j_{k-1})}(F,G)$ とおく. $\hat{A}_{\tau}^{(k-1)}=|\hat{N}_{\tau}^{(k-1,j_{k-1})}|$ とおき, 行列 H を次式で定義する.

$$H=\left(H_{p,q}\right)=N^{(j)}\left(\hat{A}^{(k-1)}(x),\frac{d}{dx}\hat{A}^{(k-1)}(x)\right), \tag{11}$$

ここに $\hat{A}^{(k-1)}(x)=\hat{A}_{j_{k-1}}^{(k-1)}x^{j_{k-1}}+\cdots+\hat{A}_0^{(k-1)}x^0$ である. $\hat{N}_{\tau}^{(k-1,j_{k-1})}$ は $\hat{N}_U^{(k-1,j_{k-1})}$ と最下部の行ベクトルから構成されるので, $\hat{N}_U^{(k-1,j_{k-1})}=\left(U^{(k)}|\boldsymbol{v}^{(k)}\right)$ （ただし $U^{(k)}$ は正方行列, $\boldsymbol{v}^{(k)}$ は列ベクトル）と表し, 最下部の行ベクトルを $\left(\boldsymbol{b}_{p,q}^{(k)}\,\middle|\,g_{p,q}^{(k)}\right)$ （ただし $\boldsymbol{b}_{p,q}^{(k)}$ は行ベクトル, $g_{p,q}^{(k)}$ は数）と表すと, $H_{p,q}$ は次式の行列式で表される.

$$H_{p,q}=\left|\begin{array}{c|c} U^{(k)} & \boldsymbol{v}^{(k)} \\ \hline \boldsymbol{b}_{p,q}^{(k)} & g_{p,q}^{(k)} \end{array}\right|, \tag{12}$$

なお, $H_{p,q}=0$ の要素に対しては, $\boldsymbol{b}_{p,q}^{(k)}=\boldsymbol{0},\ g_{p,q}^{(k)}=0$ とおく. ここで, 行列 $U^{(k)}$ は非特異であると仮定する.

このとき, $p=1,\ldots,n_1^{(k)}+n_2^{(k)}-j$ および $q=2,\ldots,n_1^{(k)}+n_2^{(k)}-j$ に対し, 行ベクトル $\boldsymbol{x}_{p,q}^{(k)}$ を, 連立 1 次方程式

$$\boldsymbol{x}_{p,q}^{(k)}U^{(k)}=\boldsymbol{b}_{p,1}^{(k)}-\boldsymbol{b}_{p,q}^{(k)} \tag{13}$$

の解により定義し, $h_{p,q}^{(k)}$ を

$$h_{p,q}^{(k)}=\boldsymbol{x}_{p,q}^{(k)}\boldsymbol{v}^{(k)} \tag{14}$$

とおく. そして, 行列 $\hat{N}^{(k,j)}(F,G)$ を次式で定義する.

$$\hat{N}^{(k,j)}(F,G)=\begin{pmatrix} U^{(k)} & v^{(k)} & v^{(k)} & \cdots & v^{(k)} \\ b_{1,1}^{(k)} & g_{1,1}^{(k)} & h_{1,2}^{(k)} & \cdots & h_{1,J_{k,j}}^{(k)} \\ b_{2,1}^{(k)} & g_{2,1}^{(k)} & h_{2,2}^{(k)} & \cdots & h_{2,J_{k,j}}^{(k)} \\ \vdots & \vdots & \vdots & & \vdots \\ b_{I_{k,j},1}^{(k)} & g_{I_{k,j},1}^{(k)} & h_{I_{k,j},2}^{(k)} & \cdots & h_{I_{k,j},J_{k,j}}^{(k)} \end{pmatrix}. \tag{15}$$

ここに

$$\begin{aligned} I_{k,j} &= n_1^{(k)}+n_2^{(k)}-j=(2j_{k-1}-2j-1)+j, \\ J_{k,j} &= n_1^{(k)}+n_2^{(k)}-2j=2j_{k-1}-2j-1 \end{aligned} \tag{16}$$

である.

このとき, $\hat{N}^{(k,j)}(F,G)$ を F と G の (k,j) **次の簡約入れ子部分終結式行列**と呼ぶ. ∎

命題 12
$k=1,\ldots,t$ および $j<j_{k-1}-1$ に対し, (k,j) 次の簡約入れ子部分終結式行列 $\hat{N}^{(k,j)}(F,G)$ の行数と列数は, それぞれ $(m+n-2(k-1)-2j)+j$ 行 $(m+n-2(k-1)-2j)$ 列である.

証明 Terui [7] を参照. ∎

命題 12 が示すように, 簡約入れ子部分終結式行列の次数は, 再帰的な部分終結式行列の次数に比べて大幅に小さくなっている (命題 5 を参照).

定義 13 (簡約入れ子部分終結式 (Reduced Nested Subresultant))
F と G をそれぞれ式 (3) で与えられる多項式とし, $(P_1^{(1)},\ldots,P_{l_1}^{(1)},\ldots,P_1^{(t)},\ldots,P_{l_t}^{(t)})$ を F と G の完全な再帰的な多項式剰余列とする. そして, 数の組 (k,j) (ただし $k=1,\ldots,t$, $j=j_{k-1}-2,\ldots,0$) および $\tau=j,\ldots,0$ に対し, (k,j) 次の簡約入れ子部分終結式行列 $\hat{N}^{(k,j)}(F,G)$ の上部 $m+n-2(k-1)-2j-1$ 行および第 $(m+n-2(k-1)-j-\tau)$ 行からなる小行列を $\hat{N}_\tau^{(k,j)}=\hat{N}_\tau^{(k,j)}(F,G)$ とおく ($\hat{N}_\tau^{(k,j)}(F,G)$ は正方行列であることに注意). このとき, 多項式

$$\hat{\mathrm{S}}_{k,j}(F,G)=|\hat{N}_j^{(k,j)}|x^j+\cdots+|\hat{N}_0^{(k,j)}|x^0 \tag{17}$$

を F と G の (k,j) **次の簡約入れ子部分終結式**と呼ぶ. ∎

入れ子部分終結式と簡約入れ子部分終結式との関係は, 次の定理によって示される.

定理 14
F と G をそれぞれ式 (3) で与えられる多項式とし, $(P_1^{(1)},\ldots,P_{l_1}^{(1)},\ldots,P_1^{(t)},\ldots,P_{l_t}^{(t)})$ を F と G の完全な再帰的な多項式剰余列とする. $k=2,\ldots,t$, $j=j_{k-1}-2,\ldots,0$ に対し, $J_{k,j}$ を式 (15) で定め, $\hat{B}_{k,j}$ と $\hat{R}_k$ をそれぞれ

$$\hat{B}_{k,j}=|U^{(k)}|^{J_{k,j}-1},\quad \hat{B}_k=\hat{B}_{k,j_k},\quad \hat{B}_1=\hat{B}_2=1, \tag{18}$$

$$\hat{R}_k=(\hat{R}_{k-1}\cdot\hat{B}_{k-1})^{J_{k,j_k}},\quad \hat{R}_1=\hat{R}_2=1 \tag{19}$$

とおく. このとき

$$\tilde{\mathrm{S}}_{k,j}(F,G)=(\hat{R}_{k-1}\cdot\hat{B}_{k-1})^{J_{k,j}}\hat{B}_{k,j}\cdot\hat{\mathrm{S}}_{k,j}(F,G). \tag{20}$$

が成り立つ. ∎

定理 14 は次の補題によって証明される.

補題 15

$k=1,\ldots,t$, $j=j_{k-1}-2,\ldots,0$, $\tau=j,\ldots,0$ に対し,

$$|\tilde{N}_{\tau}^{(k,j)}(F,G)| = (\hat{R}_{k-1}\cdot\hat{B}_{k-1})^{J_{k,j}}\hat{B}_{k,j}|\hat{N}_{\tau}^{(k,j)}(F,G)|. \tag{21}$$

が成り立つ.

証明 $|\tilde{N}_{\tau}^{(k,j)}(F,G)|$ に対し, 分数なし Gauss の消去法 [1] を適用することによって示される. 詳細は Terui [7] を参照. ∎

5 まとめ

本稿では, 1 変数多項式の部分終結式の拡張の一つである再帰的な部分終結式の新たな表現として, 入れ子部分終結式および簡約入れ子部分終結式を与えた. 入れ子部分終結式は, 終結式行列が, 従来の部分終結式の係数を表す行列式の入れ子の形の表現で与えられ, 再帰的な部分終結式とは符号を除いて等しいことを示した. 簡約入れ子部分終結式は, 入れ子部分終結式行列を分数なし Gauss の消去法で簡約したものと同値になり, 行列の次元が再帰的な部分終結式行列に比べて大幅に小さくなくことを示した.

参 考 文 献

[1] E. H. Bareiss. Sylvester's identity and multistep integer-preserving Gaussian elimination. *Math. Comp.*, Vol. 22, pp. 565–578, 1968.

[2] W. S. Brown and J. F. Traub. On Euclid's Algorithm and the Theory of Subresultants. *J. ACM*, Vol. 18, No. 4, pp. 505–514, 1971.

[3] G. E. Collins. Subresultants and Reduced Polynomial Remainder Sequences. *J. ACM*, Vol. 14, No. 1, pp. 128–142, 1967.

[4] D. Knuth. *The Art of Computer Programming*, Vol. 2: Seminumerical Algorithms. Addison-Wesley, Third edition, 1998.

[5] R. Loos. Generalized polynomial remainder sequences. In B. Buchberger, G. E. Collins, and R. Loos, editors, *Computer Algebra: Symbolic and Algebraic Computation*, pp. 115–137. Springer-Verlag, Second edition, 1983.

[6] A. Terui. Subresultants in recursive polynomial remainder sequence. In V.G. Ganzha, E.W. Mayr, and E.V. Vorozhtsov (eds.), *Proc. CASC 2003*, pp. 363–375, München, 2003. Institute für Informatik, Technische Universität München.

[7] A. Terui. Recursive polynomial remainder sequence and the nested subresultants. In V.G. Ganzha, E.W. Mayr, and E.V. Vorozhtsov (eds.), *Proc. CASC 2005*, LNCS 3718, pp. 445–456. Springer, 2005.

[8] J. von zur Gathen and T. Lücking. Subresultants revisited. *Theoret. Comput. Sci.*, Vol. 297, No. 1-3, pp. 199–239, 2003. Latin American theoretical informatics (Punta del Este, 2000).

[9] 照井章. 再帰的な部分終結式と 1 変数代数方程式の実根の個数の計算. 数理解析研究所講究録 1395 *"Computer Algebra—Algorithms, Implementations and Applications"*, pp. 97–103. 京都大学数理解析研究所, 2004.